DEPARTMENT OF THE AIR FORCE
WASHINGTON DC 20330

MORANDUM FOR ALMAJCOM/FOA/DRU/SFI

12 Jul 04

FROM: HQ USAF/XOFI
1340 Air Force Pentagon
Washington, DC 20330-1340

SUBJECT: AF Joint Personnel Adjudication System (JPAS) Guide

The attched AF JPAS Guide has been developed to define the different JPAS applications, system configuration as well as to identify and explain each authorized user level. The guide will be posted at our website at https://wwwmil.lackland.af.mil/afsf/. We will update the guide as new JPAS releases occur. Thank you for your help in developing the guide.

Our POC is Ms Cynthia Smith-Rainey AF/XOFI, DSN 425-0010, email: cynthia.smithrainey @pentagon.af.mil.

DANIEL E. BISHOP
Chief, Information Security Division
Directorate of Security Forces

Attachment
AF JPAS Guide

cc:
AF/XOF
AFCAF/PS
AF/DPPH
AF/ILV

Air Force Joint Personnel Adjudication System (JPAS) Guide

I. Description:

JPAS is the Department of Defense (DoD) personnel security clearance and access database. It facilitates personnel security management for the DoD Central Adjudication Facility (CAFs), security managers and officers both non-SCI and SCI functions. It interfaces with the investigative providers, the personnel systems within the Department thus eliminating manual transactions and expediting the flow of personnel security information to warfighters. JPAS is operated and maintained by the Air Force on behalf of the DoD Components and USD/I.

II. Structure:

JPAS has two applications:

The Joint Adjudication Management System (JAMS) is for adjudicative personnel only and provides capabilities such as case management/distribution, adjudication history and summary, due process, revocations, and denial action, and the ability for each CAF to electronically access investigative reports from the investigative providers.

Joint Clearance and Access Verification System (JCAVS) is for non-SCI and SCI security managers/officers and provides capabilities such as access indoctrination/debriefing history, incident/issue file reporting, history and management of unit personnel security functions.

JPAS will use a centralized database with centralized computer processing and application programs for standardized DoD personnel security processes.

JPAS automates both core and CAF-unique functionality and provides "real-time" information regarding clearance, access and investigative status to authorized DoD security personnel and other interfacing organizations, such as Defense Security Service, Defense Manpower Data Center, Defense Civilian Personnel Management System, Office of Personnel Management, Air Force Personnel Center.

Telecommunications and automated information systems interface software will serve as the cornerstone for the CAFs virtual consolidation and ensure re-engineering of core personnel security and adjudication processes.

All dates in JCAVS are entered YYYY MM DD.

III. System Configuration:

Pentium 133 MHZ or Better
150 MB Free Disk Space
128 MB RAM (Minimum)

Windows 95/Windows NT or Later
Netscape 4.7 or Higher is DoD/AF Approved Browser, JPAS is now Browser neutral

Ensure Port #443 and #80 are open (Port #443 allows entry to JPAS and Port #80 allows internet access). Browser must have 128-BIT encryption and DNS reverse hook up must be enabled. JPAS will allow .MIL/.GOV/.COM domains through its firewall.

JPAS is a web base system on NIPRNET. Bookmark JPAS Gateway Home Page at HTTPS://JPAS.OSD.MIL. This page provides daily updates, notification of downtime as well as updates on system enhancements. Logon via JPAS Gateway Home Page. Contact the Help Desk DSN 754-2924/2904 or 297/9444 for technical questions and your Account Manager (AM) for functional questions.

IV. Becoming a JPAS User:

Air Force designated in each MAJCOM a Primary and Alternate AM. This is usually the Security Forces. AMs can create accounts and designate other AMs. AMs are responsible for creating an Access Request Form (ARF) to designate JPAS Users. AMs will maintain original ARFs for all levels created. JPAS User level access is determined by the AM. The following outlines the different User levels and investigation required.

Level 2 - SCI security personnel at unified command, DoD agency, military installation or major command/equivalent headquarters. PSM - Net is determined by the responsible SOIC or designee. (Read and Write Access - SSBI/DCID 6/4 with current SCI Access) **M-1 Criteria.

Level 3 - SCI security personnel at echelons subordinate to Level 2 at a particular geographic location (installation, base, post, naval vessel). PSM - Net is determined by the responsible SOIC or designee. (Read and Write Access-SSBI/DCID 6/4 with current SCI Access) **M-1 Criteria.

Level 4 - Non-SCI security personnel at unified command, DoD agency, military department or major command/equivalent headquarters. PSM - Net is determined by the responsible Security Officer or designee. (Read and Write Access - NACLAC/ANACI/Secret Eligibility)

Level 5 - Non-SCI security personnel at echelons subordinate to Level 4 at geographic location (installation, base, post, naval vessel). PSM - Net is determined by the responsible Security Officer or designee. (Read and Write Access - NACLC/ANACI/Secret Eligibility)

Level 6 - Unit Security Manager (additional duty) responsible for security functions as determined by responsible senior security official. (Read and Write Access - NACLC/ANACI/Secret Eligibility)

Level 7 - Non-SCI Entry Control Personnel. Individuals who grant access to installations, buildings, etc. Varies according to organizations. (Read Access - NACLC/ANACI/Secret Eligibility)

Level 8 - SCI Entry Control Personnel. Individuals who grant access to SCIF installations, buildings, etc. Varies according to organizations. (Read Access - SSBI/DCID 6/4 Eligibility)

Level 10 - Visitor Management. Level 10 users will have the same view of the JCAVS Personnel Summary as a JCAVS Level 7 User. They will receive Visit Notification when their SMO is being notified of a visit. A Level 10 User may **not** be an AM create or delete an account at any level. NACLC/ANACI/Secret Eligibility.

To unlock or reset passwords Users must contact their AM.

Future New User Level. DoD approved a new User Level 9 - Suitability (Fields still under development)

Designated users have authority to read/write limited fields that reflect a suitability/trustworthiness determination. These are positions of trust, non-sensitive positions, trustworthiness positions, that do not require access to classified information, but require an investigation. Such users are usually from Human Resource Offices, Civilian Personnel Offices, etc. The fields accessed are name, SSAN, DOB, POB, date of submission of investigation, date opened, date closed, results of investigation/suitability determination. Users can access links to indoctrinate, research/recertify/upgrade, ESPQ, incident report, in/out process, add/modify suitability history, investigation history, adjudication history. (Limited Read and Write Access - NACLC/ANACI)

Ad Hoc Reporting Reporting. Authorized users view and produce summary level reports by selecting combining and/or filtering data elements of a given report type. The report database includes only active persons and is updated twice a week. JPAS ad hoc reports include:

Person Eligibilities
Investigations
Case Assigned
Cases Awaiting Action
Cases in Progress
Cases Closed
Accesses

V. Security Management Office (SMO):

Log on as an AM and go to "Maintain SMO"
Click SMO code box, using your PASCODE. Once your PASCODE is listed click on SMO code. The system will bring up your office information.

If at any time you forget to click "Save" you will be required to repeat the above steps for setting up a SMO.

VI. Personnel Security Management (PSM):

PSM Net is the creation of a network through the establishment of a relationship between an SMO and the personnel it serves. These relationships are categorized as either Owning or Serving. PSM Net is based on the concept that every person will belong (Owned) by one SMO for collateral (Non-SCI) clearances and one SMO for SCI clearances. Additionally, a person may be serviced by any number of SMO's. A servicing relationship is anything other than an owning relationship. It reflects the capability to provide security services on a temporary basis outside the person's permanent unit or organization. Example: Provide security services for a school assignment, individual permanently certified to work at your facility due to TDY etc. The business rule for routing all security notifications will be based on the owning and servicing relationship. The government does not "own" an industry employee. The government provides a "service" by authorizing them access to specific types of information.

Log on as a User Level 2-6. If you have more than one category or more than one user level the Choose Category/Level screen populates upon login. Select your Category and User level and click the OK button. The Welcome Screen populates with the main menu on the left side of the screen. Select the PSM Net Link. This will take you to the screen titled JCAVS maintain PSM Net. Your SMO will appear on the top line.

When your SMO is displayed on the top line if your PSM Net is already established there should be a list of names under person categories. If your PSM Net is not established click the Person Categories by Organization radio button, then click the ADD button. The PSM Net Add Person Categories screen populates. Select the relationship (Owning/Servicing). Click the select Organization button and the Organization Search screen populates. Search for the organization and click OK. The PSM Net Add Person Categories screen populates with the organization. Click the Search button. All personnel assigned to the organization will populate under Search Results. Choose the Add All button and all person categories for the organization will be added to your PSM Net.

To remove person categories from your net, click the PSM Net link choose the person category from the JCAVS Maintain PSM Net screen and check the Remove radio button and click save. To remove SMOs select the "Remove" button and view the list of PASCODES. Note: This removes all categories for that organization owned and serviced. Check the remove box for organization to be removed and click the Save button. This action will place pending removals in the relationship column after you save. Remember to click the "Save" button at the end of each page. Personnel and/or commands selected will be "Removed" off your list daily at midnight (Eastern Standard Time).

After removing all personnel not owned or serviced under your PSM Net use your PASCODE to add person categories by organization. You should own everyone permanently attached to your command and service personnel falling into the category identified previously.

You can also take an owning or servicing relationship using the Person Summary Screen. Click "Select Person" link and enter SSAN. Click on the "In or Out" process link.

Setting and maintaining your office PSM Net will keep the network current and enable delivery of AFCAF Notifications, provide accurate reports and aid in overall system performance.

VII. SCI Specific:

Ensure the proper person category is selected for personnel with multiple categories (Example: Civilian, Contractor, or Reservist). When entering SCI access information enter the individual's SSAN and click display. Click on the drop down arrow menu to select the person categories. Once selected, you can "In or Out" process the member. For the indoctrination link to appear the person must meet the eligibility requirements and the person must be in your PSM Net.

VIII. Person Summary Screen (Entering and/or Updating):

The Non-Disclosure Agreement (Non-SCI) - NDA SF 312 must be executed and entered prior to any other indoctrination action. If there is no record or date is not listed on Person Summary Screen within JCAVS a new NDA must be executed.

Non-Disclosure Statement (NDS) DD Form 1847-1 - SCI Data Entry. If there is no record of prior execution of the NDS DD Form 1847-1 a new NDS DD Form 1847-1 must be executed prior to entering accesses in JCAVS.

The attestation date entry field is on the Non-SCI section of the screen.

Indoctrination dates of accesses (SI/TK/G/HCS etc.) will be entered.

The debrief link will not appear until indoctrination has been accomplished and will appear only for those accesses held. Debrief dates will be entered immediately following debrief and will be annotated with the most appropriate reason for debrief from the pull down menu.

Notification:
A notification indicator (magnifying glass icon) will appear beside the links that have notifications, alerting the SMO of updates. This notification indicator is refreshed upon login when removed from notification screen by SMO staff. All JCAVS notifications will be removed automatically after 30 days. Click on SSN to view notification. If no Owner or no PSM Net is established, notifications will not be sent to SMOs.

Request to Research and Upgrade Link (RRU) - Only one RRU can be completed at a time on individual categories. A second request cannot be submitted until the first request is answered by the AFCAF. Once AFCAF responds (sending a notification back to the SMO), the SMO will be able to send another RRU to the AFCAF, if needed for that person.

All official travel will be entered for personnel in access. Only User Level 2 and 3 may enter unofficial travel.

JPAS has no Transfer In Status (TIS) function.

NOTE FUTURE REQUIREMENTS:

1. Standard Form (SF) 714, Financial Disclosure. DoD will implement the SF 714 in the future. Users will input data fields concerning execution of the form into JPAS on particular categories of people with regular access to certain types of information as specified in Section 1.3 of Executive Order 12968, Access to Classified Information. Pending DoD implementation.

2. New User Level 9. DoD approved a new User Level 9 - Suitability Determinations. Pending final development of User 9 fields.